


view of "Applied Cryptography", pages 38-39, by Schneier ("Schneier"). No mention is made as to the reasoning for rejecting Claim 14, nor is it mentioned as rejected on other than the summary page of the Office Action. 

Aziz shows a system for performing a secure login of a user on a server. In operation, a user provides a login address and a password at a client workstation 40 (see, FIG. 5, and the accompanying text contained in Col. 6, lines 4-8). The login address and the password are provided to the server and are checked by the server against a list of authorized users (see, Col. 6, lines 14-16). If the identified user is an authorized user, the server produces a random number that is encrypted using a standard privacy enhanced mail (PEM) public key. The server then places the encrypted random number in a user directory (see, Col. 6, lines 20-26). The user requests transfer of the encrypted random number using file transfer protocol (ftp). At the workstation, the encrypted random number is decrypted using the user's private key which is apparently stored at the user's workstation. (See, Col. 6, lines 41-43!). The random number is then sent back to the server in an unencrypted form where it is compared to the stored random number to give access to the server by the user's workstation. In this was, a user's login to the server is authenticated.

It must be stressed and understood that at no time is the private key of the user transmitted to the user by the server. In fact the random number is not maintained for further cryptographic operations and in fact is not used in any capacity as a private key. As stated in Aziz, in fact the random number even has an expiration date wherein if the user does not complete the login by a specified time period, the random number will expire (see, Col. 6, line 66 through Col. 7, line 2).

This random number is in no way a private key as is understood by a person of ordinary skill in the art or as described in Aziz. As discussed in Aziz (emphasis provided), "[s]ince RSA technology is well known, it will not be described further herein." Private key is a term of art that is well understood by a person of ordinary skill and would not be understood to serve the function described in Aziz. This use of the private key term of art clearly is understood within Aziz (see, Col. 6, 41-51 of Aziz).

As described within the present patent application on page 1, lines 9-22, "[p]ublic key cryptosystems in which a pair of a corresponding public key and a private (or secret) key is assigned for each user can be used in a variety of applications in a networked environment. In such applications, a private key can be used for encryption or for decryption solely by or on behalf of the assigned user. One use of a private key for encryption is to produce a digital signature of a digital document (for all purposes in this application the term

"document" is intended to include any message, file, program or other data) on behalf of a user to manifest the user's modification, or review, and approval of the modified and/or reviewed document or otherwise indicate that the user is the source of the document (hereafter "approved document")."

As is understood by a person of ordinary skill in the art, the private key is utilized for cryptographic functions such as encryption and decryption of documents. This private key must be kept secured otherwise the cryptographic system fails since unauthorized parties that obtain the private key could pass themselves off as the legitimate private key holder.

This is the problem that is addressed by the present invention. Please refer to the description of operation of the present invention fully described in the Amendment submitted on January 5, 2000. In the present invention, the private key is not stored at the user site and therefor is not available to an unauthorized user (see, Page 13, line 28 through Page 14, line 1). Aziz does not address this problem in any form.

Particularly, Aziz does not disclose or suggest (emphasis provided) "reading from a storage means data corresponding to the user having the received ID, which data comprises the user's private key encrypted using a key determined from identifying information of the user; and sending via the network the encrypted private key, whereby the encrypted private key can be received and decrypted at the location of the user" as required by Claim 1. Further, Claims 5 and 11 also substantially require these inventive elements and therefore are allowable for similar reasons.

Schneier merely provides a description of an authentication procedure using a hashing operation wherein a hash of a document is encrypted using a private key. The result is transmitted to a second party and is decrypted using a corresponding public

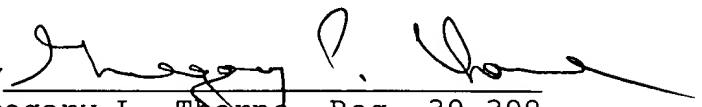
key. The hash of the document is then compared to the stored hash of the document to complete the authentication process. This operation is also described in the present patent application in the Background of the Invention (e.g., prior art section) in Page 1, line 23 through Page 2, line 10.

Based on the foregoing, the Applicants respectfully submit that independent Claims 1, 5, and 11 are patentable over Aziz, and notice to this effect is earnestly solicited. Claims 2-4, 6-10, and 12-20 depend from one of Claims 1, 5, and 11, respectively, and accordingly are allowable for at least this reason.

Applicants have made a diligent and sincere effort to place this application in condition for immediate allowance and notice to this effect is earnestly solicited.

Early and favorable action is earnestly solicited.

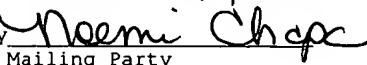
Respectfully submitted,

By 
Gregory L. Thorne, Reg. 39,398
Attorney
(914) 333-9665
June 16, 2000

CERTIFICATE OF MAILING

It is hereby certified that this correspondence is being deposited with the United States Postal Service as first-class mail in an envelope addressed to:

COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

On June 16, 2000
By 
Mailing Party